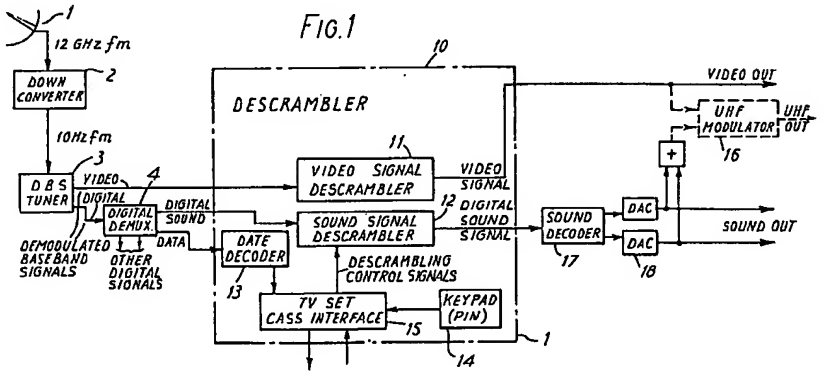
(12) UK Patent Application (19) GB (11) 2 132 860 A

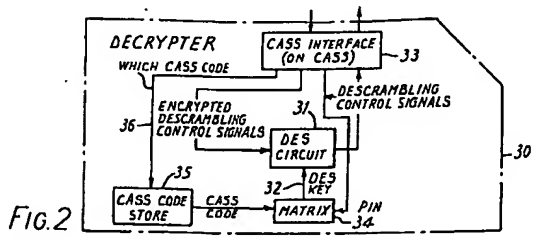
(21) Application No 8333987
(22) Date of filing 21 Dec 1983
(30) Priority data
(31) 8236350
8313295
(32) 21 Dec 1982
13 May 1983
(33) United Kingdom (GB)
(43) Application published
11 Jul 1984
(51) INT CL³
H04K 1/00
H04N 7/16
(52) Domestic classification
H4R 22C 22V PTS
(56) Documents cited
GB A 2067871
GB 1602119
GB 1475743
EP A1 0018869
Specifications WO A1
80/02901
WO 80/00209
(58) Field of search
H4R
H4F

(71) Applicant
British Broadcasting Corporation,
(United Kingdom),
Broadcasting House,
London W1A 1AA.
(72) Inventors
John Philip Chambers,
Stanley Makinson Edwardson,
Derek Thomas Wright.
(74) Agent and/or Address for Service
Reddie & Grose,
16 Theobalds Road,
London WC1X 8PL.

(54) **Conditional-access broadcast transmission**

(57) A conditional-access television receiver includes a descrambler circuit 10 which is enabled by descrambler control signals received from a conditional access-sub-system (CASS). The descrambler control signals are derived from off-air control data signals by a decryption circuit 31 responsive to a key. The key is formed in each receiver in a matrix 34 by combining a personal identification number (PIN) with a CASS code read from a CASS store 35. The appropriate CASS code is selected by further broadcast data. Alternatively a pre-payment or direct debit accounting system can be used.

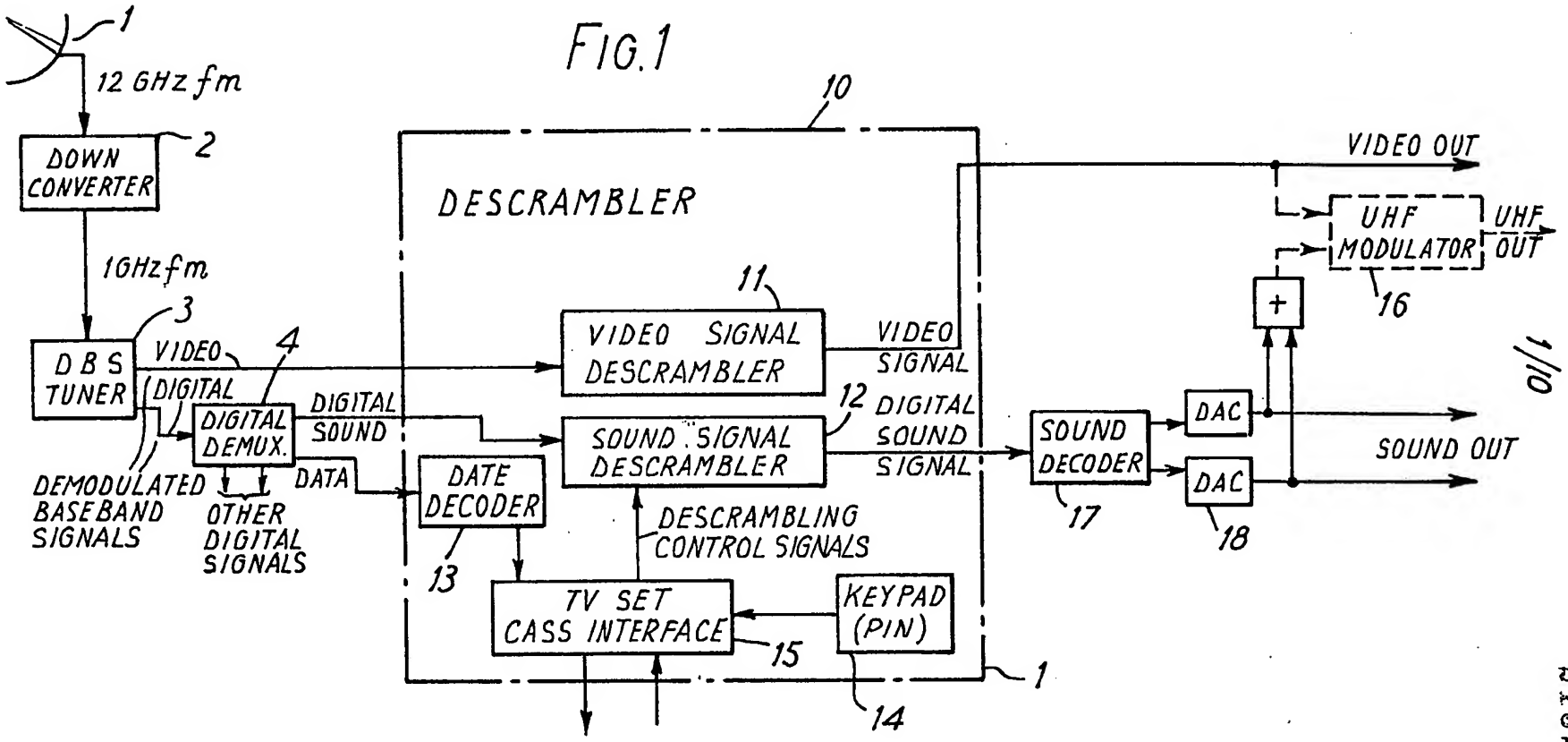




The drawing(s) originally filed was/were informal and the print here reproduced is taken from a later filed formal copy.

GB 2 132 860 A

FIG.1



1/10

2132860

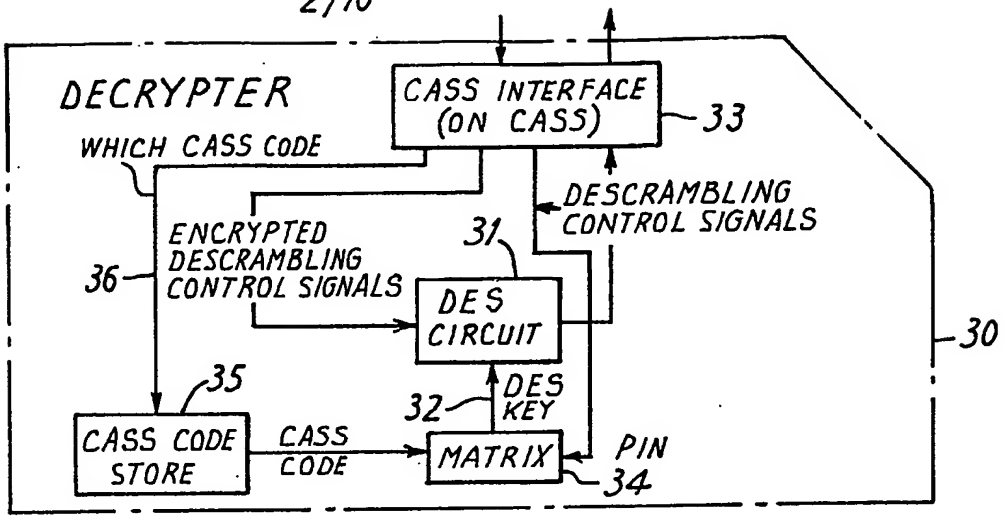


FIG.2

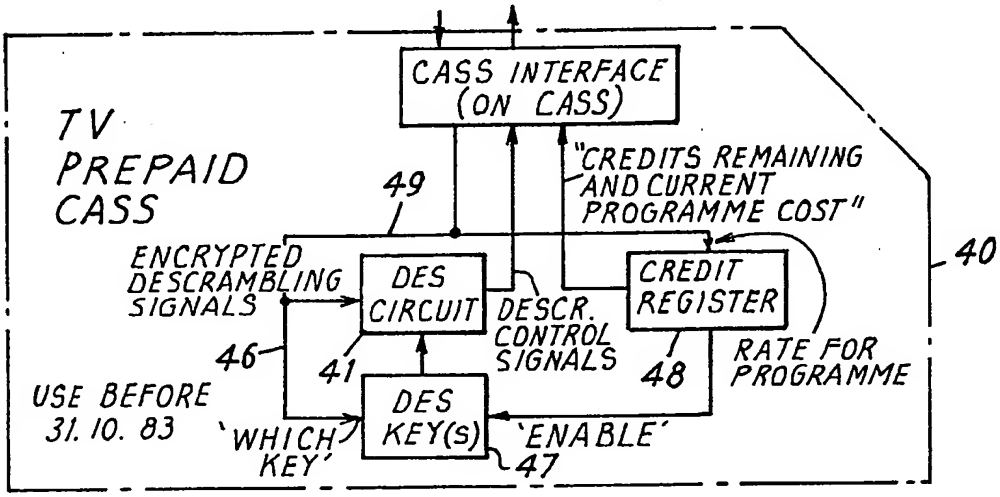


FIG.3

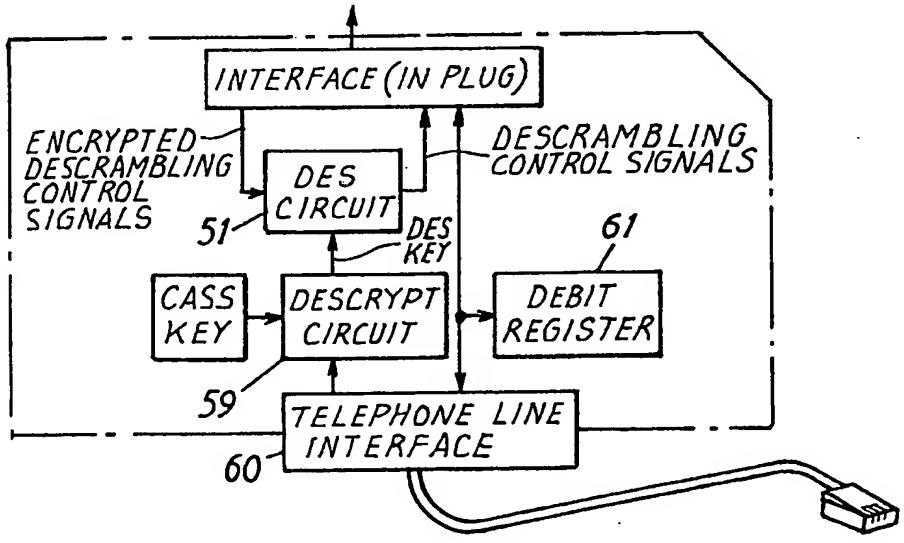


FIG.4

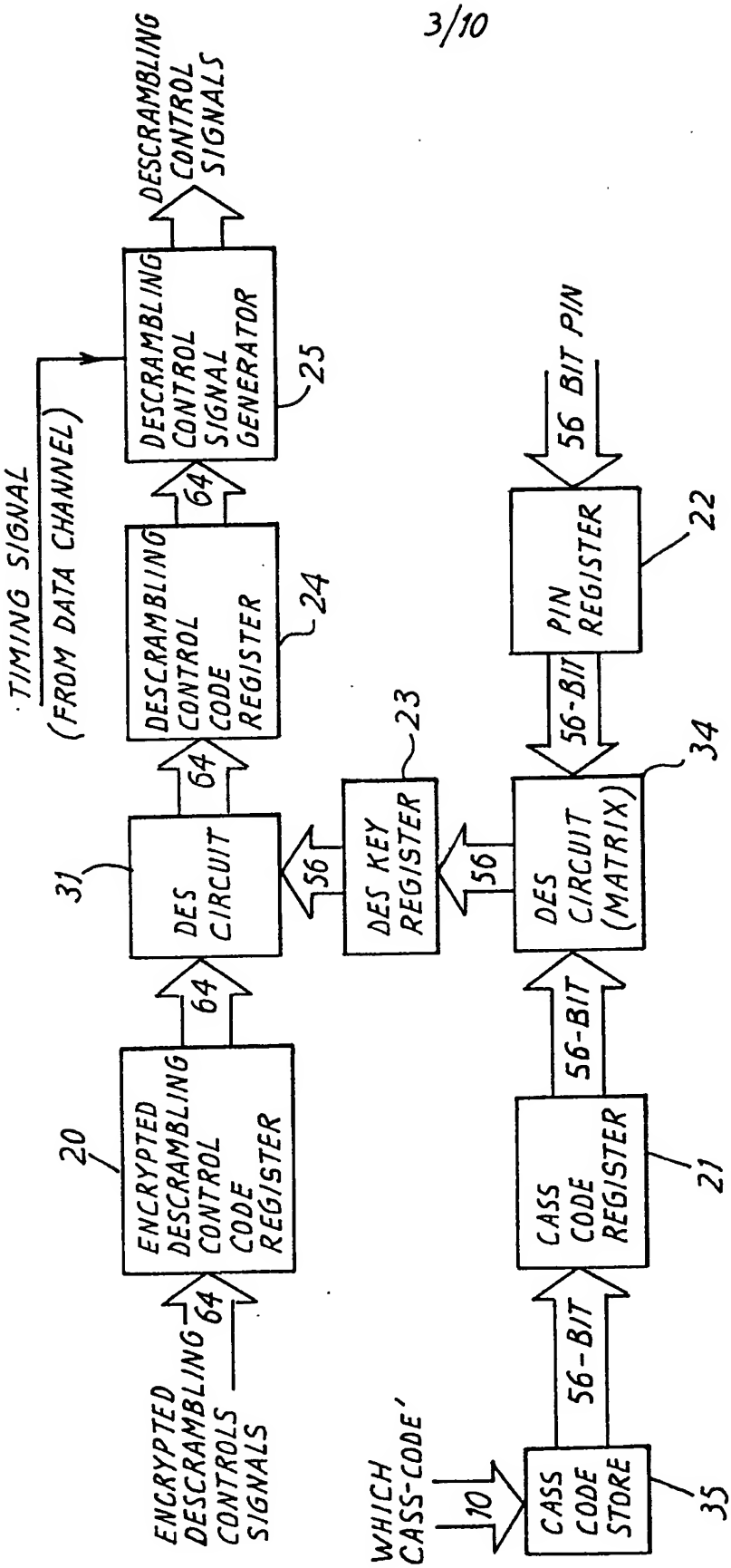

ENCRYPTED DESCRAMBLING CONTROLS SIGNALS
64
ENCRYPTED DESCRAMBLING CONTROL CODE REGISTER
20
64
31
DES CIRCUIT
64
DESCRAMBLING CONTROL CODE REGISTER
24
64
DESCRAMBLING CONTROL SIGNAL GENERATOR
25
DESCRAMBLING CONTROL SIGNALS
TIMING SIGNAL (FROM DATA CHANNEL)
56
DES KEY REGISTER
23
56
DES CIRCUIT (MATRIX)
34
56-BIT
PIN REGISTER
22
56 BIT PIN
'WHICH CASS-CODE'
10
CASS CODE STORE
35
56-BIT
56-BIT
CASS CODE REGISTER
21

FIG.5

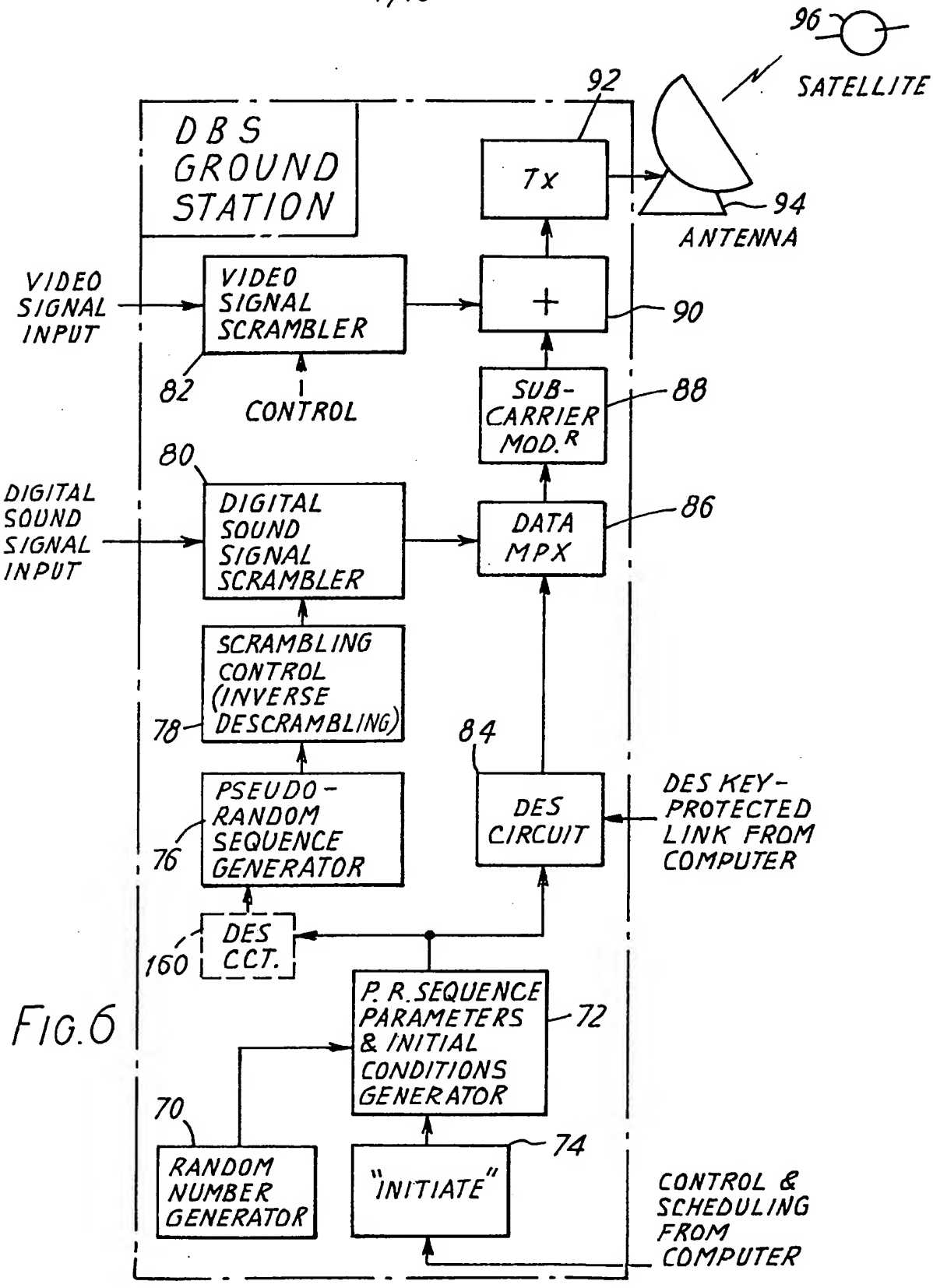

DBS GROUND STATION
96
SATELLITE
92
Tx
94
ANTENNA
VIDEO SIGNAL INPUT
VIDEO SIGNAL SCRAMBLER
+
90
82
CONTROL
SUB-CARRIER MOD.R
88
80
DIGITAL SOUND SIGNAL INPUT
DIGITAL SOUND SIGNAL SCRAMBLER
DATA MPX
86
SCRAMBLING CONTROL (INVERSE DESCRAMBLING)
78
84
PSEUDO-RANDOM SEQUENCE GENERATOR
76
DES CIRCUIT
DES KEY-PROTECTED LINK FROM COMPUTER
160
DES CCT.
P.R.SEQUENCE PARAMETERS & INITIAL CONDITIONS GENERATOR
72
70
RANDOM NUMBER GENERATOR
"INITIATE"
74
CONTROL & SCHEDULING FROM COMPUTER

FIG.6

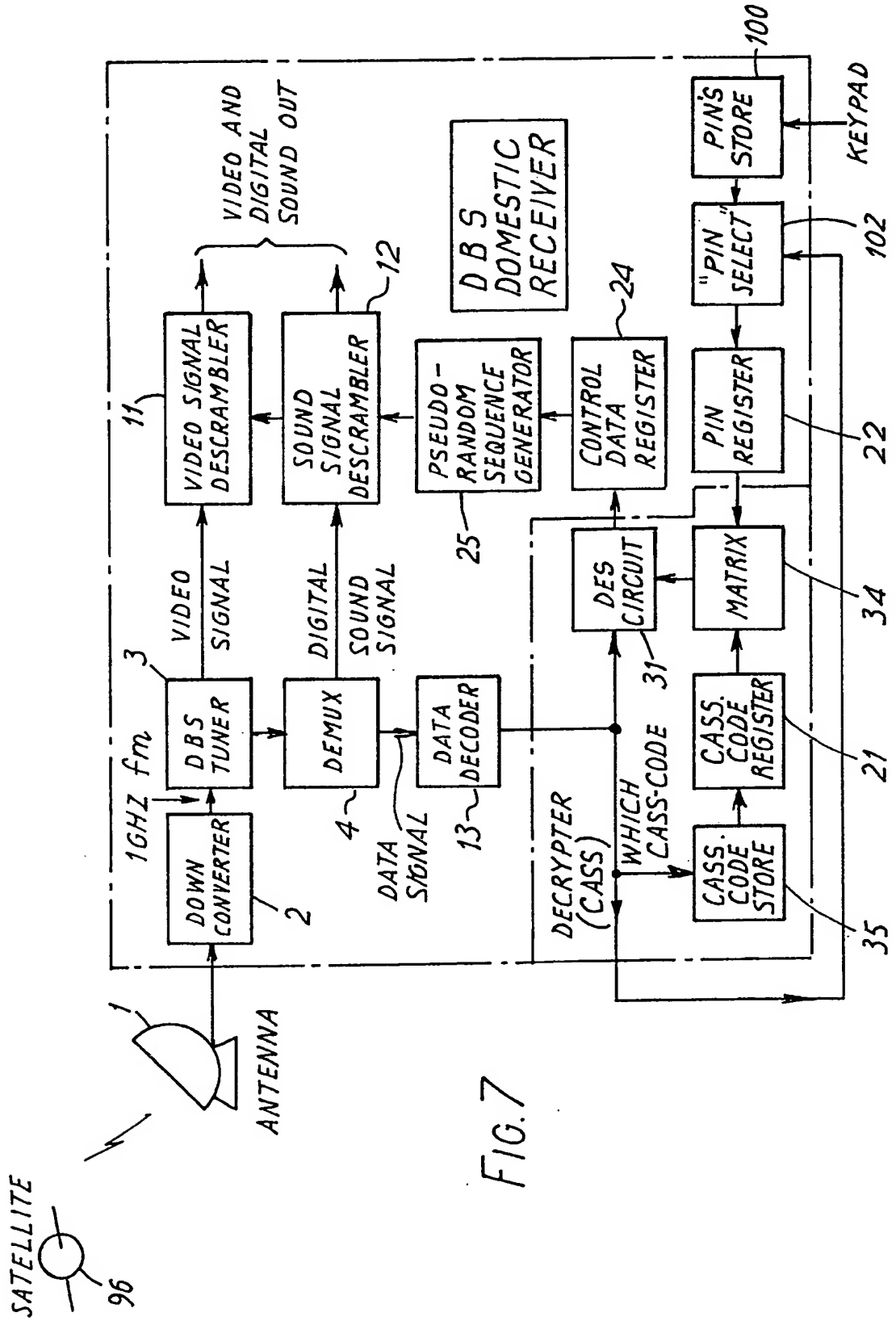

SATELLITE
96
ANTENNA
1
1GHZ fm
DOWN CONVERTER
2
DBS TUNER
3
VIDEO SIGNAL
DIGITAL SOUND SIGNAL
DEMUX
4
DATA SIGNAL
DATA DECODER
13
VIDEO SIGNAL DESCRAMBLER
11
SOUND SIGNAL DESCRAMBLER
12
VIDEO AND DIGITAL SOUND OUT
PSEUDO-RANDOM SEQUENCE GENERATOR
25
CONTROL DATA REGISTER
24
DES CIRCUIT
31
DECRYPTER (CASS)
WHICH CASS-CODE
CASS. CODE STORE
35
CASS. CODE REGISTER
21
MATRIX
34
PIN REGISTER
22
"PIN SELECT"
102
PIN'S STORE
100
KEYPAD
DBS DOMESTIC RECEIVER

FIG. 7

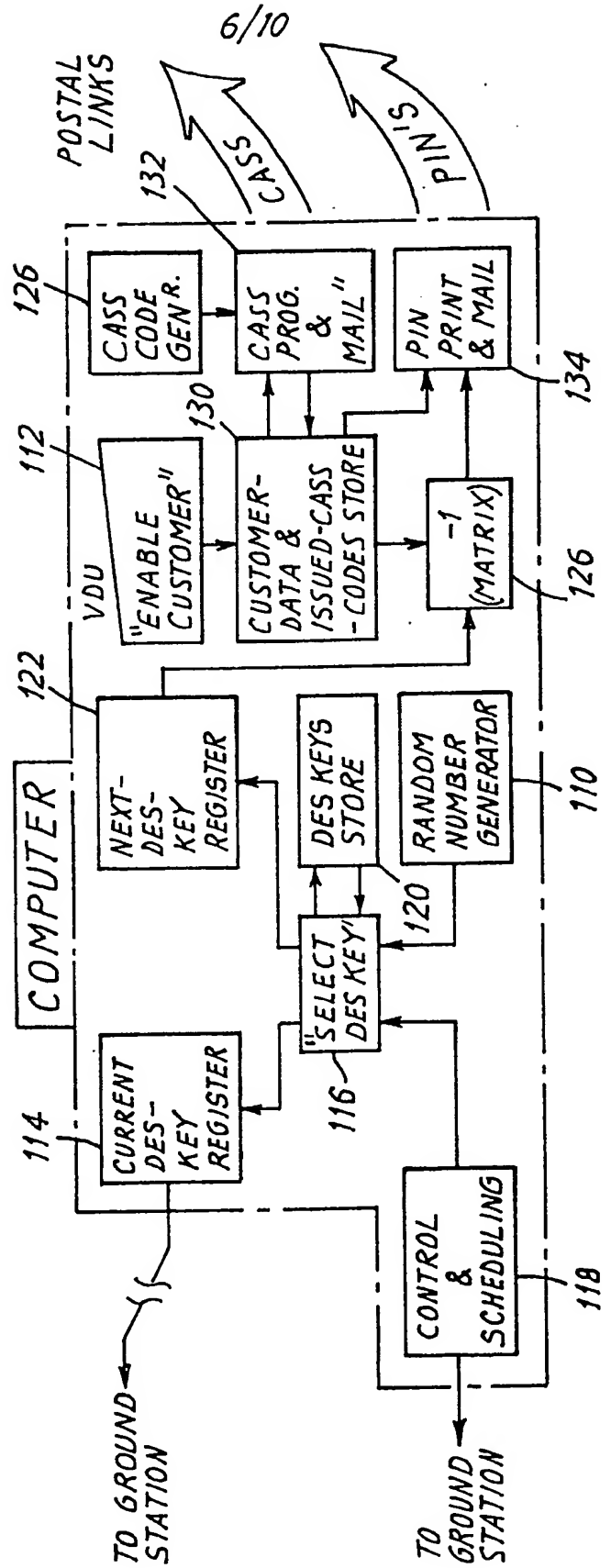

POSTAL LINKS
CASS
PIN'S
132
126
CASS CODE GEN^R.
CASS PROG. & MAIL"
PIN PRINT & MAIL
134
112
VDU
"ENABLE CUSTOMER"
130
CUSTOMER-DATA & ISSUED-CASS -CODES STORE
-1 (MATRIX)
126
122
COMPUTER
NEXT-DES-KEY REGISTER
DES KEYS STORE
RANDOM NUMBER GENERATOR
110
120
"SELECT DES KEY"
116
114
CURRENT DES-KEY REGISTER
CONTROL & SCHEDULING
118
TO GROUND STATION
TO GROUND STATION

FIG.8

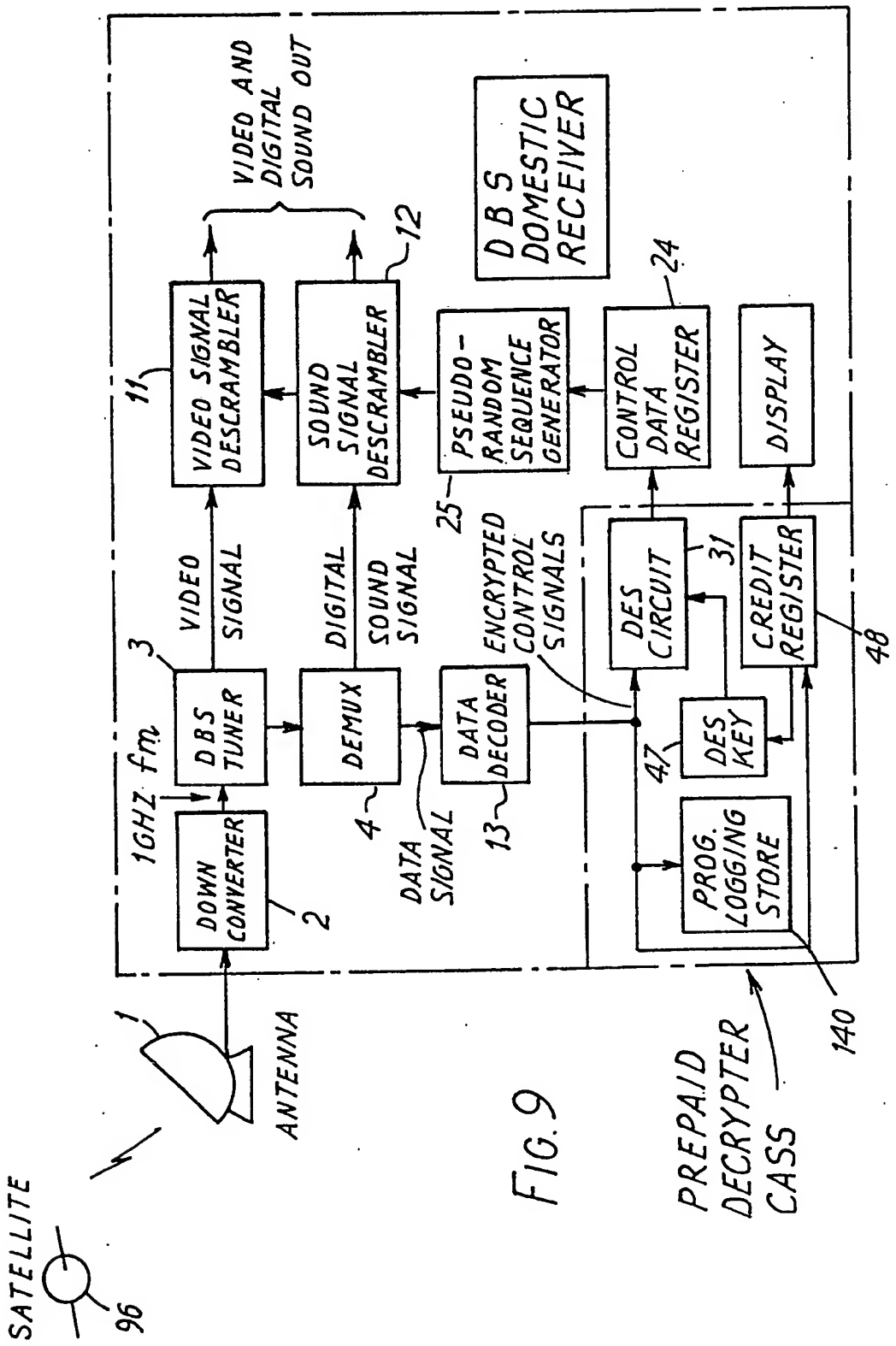

SATELLITE
96
ANTENNA
1
1GHZ fm
DOWN CONVERTER
2
DBS TUNER
3
VIDEO SIGNAL
DEMUX
4
DIGITAL SOUND SIGNAL
DATA SIGNAL
DATA DECODER
13
ENCRYPTED CONTROL SIGNALS
VIDEO SIGNAL DESCRAMBLER
11
SOUND SIGNAL DESCRAMBLER
12
VIDEO AND DIGITAL SOUND OUT
PSEUDO-RANDOM SEQUENCE GENERATOR
25
DES CIRCUIT
31
DES KEY
47
PROG. LOGGING STORE
CONTROL DATA REGISTER
24
CREDIT REGISTER
48
DISPLAY
DBS DOMESTIC RECEIVER
PREPAID DECRYPTER CASS
140

FIG. 9

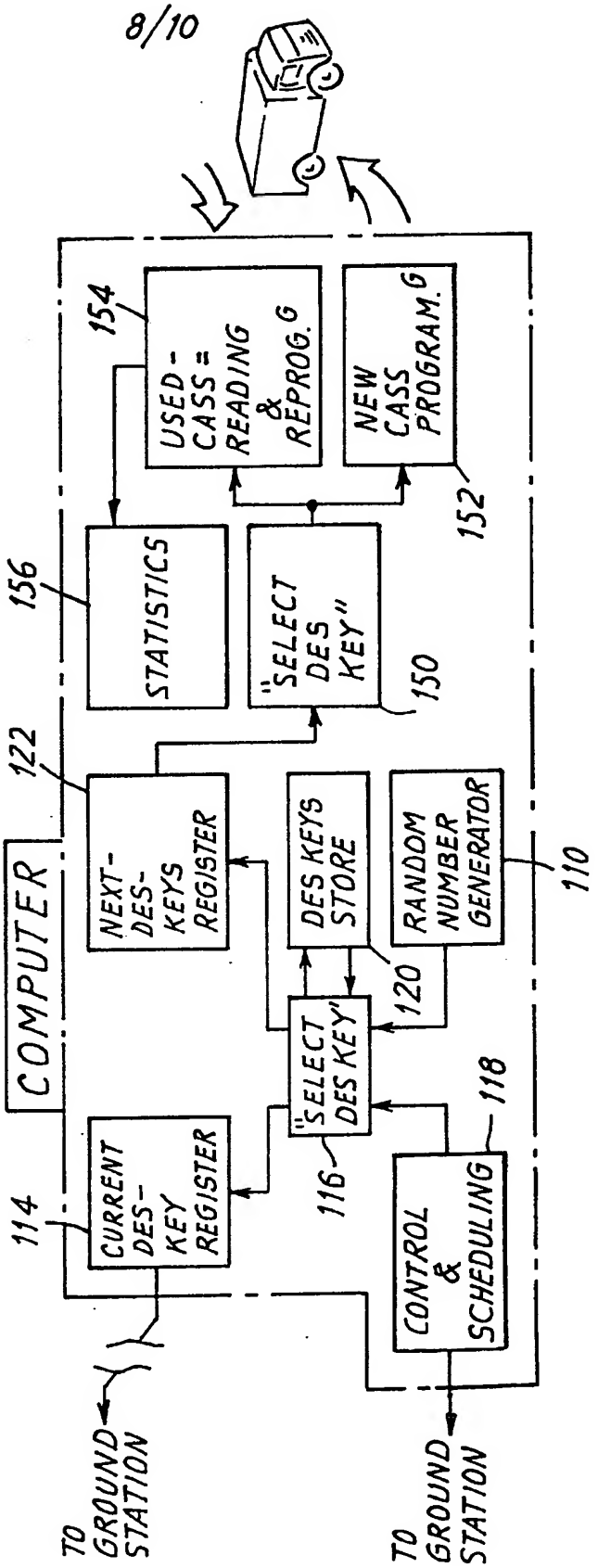

COMPUTER
114
CURRENT DES-KEY REGISTER
NEXT-DES-KEYS REGISTER
122
"SELECT DES KEY"
116
DES KEYS STORE
120
RANDOM NUMBER GENERATOR
110
CONTROL & SCHEDULING
118
"SELECT DES KEY"
150
STATISTICS
156
USED-CASS = READING & REPROG.G
154
NEW CASS PROGRAM.G
152
TO GROUND STATION
TO GROUND STATION

FIG. 10

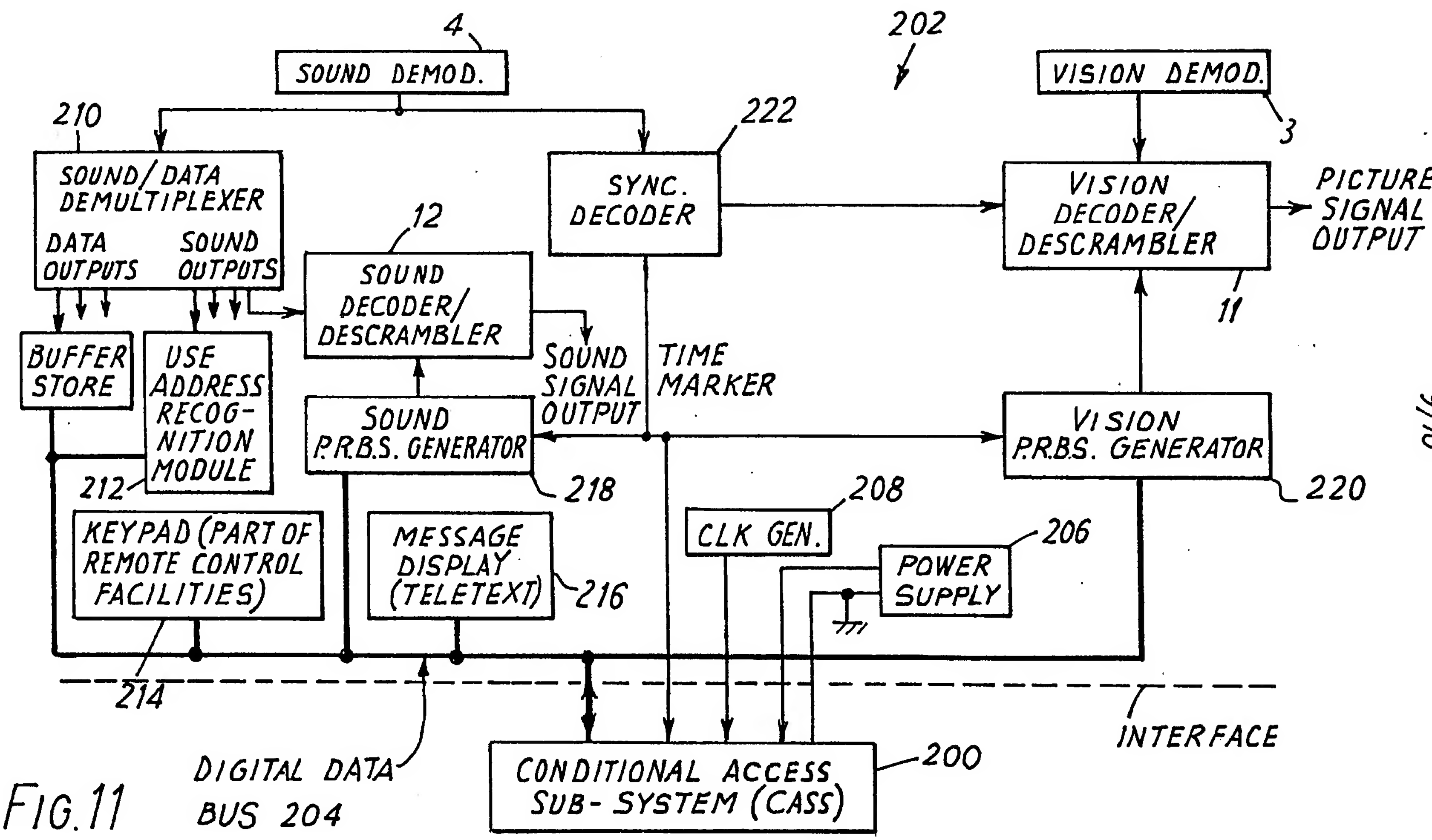

SOUND DEMOD.
4
202
VISION DEMOD.
3
210
SOUND/DATA DEMULTIPLEXER
DATA OUTPUTS
SOUND OUTPUTS
222
SYNC. DECODER
VISION DECODER/ DESCRAMBLER
PICTURE SIGNAL OUTPUT
11
12
SOUND DECODER/ DESCRAMBLER
BUFFER STORE
USE ADDRESS RECOG- NITION MODULE
212
SOUND SIGNAL OUTPUT
TIME MARKER
SOUND P.R.B.S. GENERATOR
218
VISION P.R.B.S. GENERATOR
220
KEYPAD (PART OF REMOTE CONTROL FACILITIES)
214
MESSAGE DISPLAY (TELETEXT)
216
CLK GEN.
208
POWER SUPPLY
206
INTERFACE
DIGITAL DATA BUS 204
CONDITIONAL ACCESS SUB-SYSTEM (CASS)
200

FIG.11

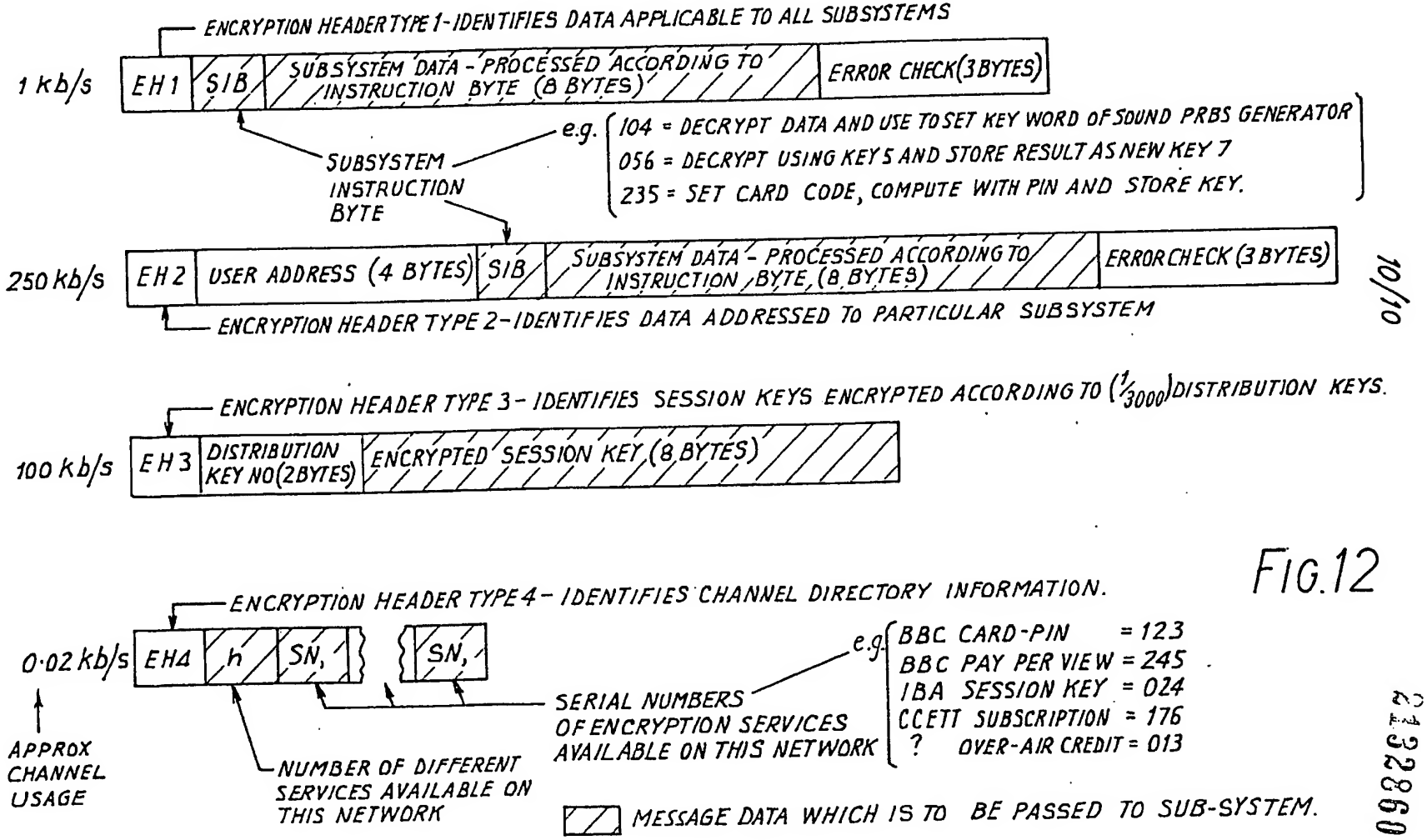


FIG.12

10/10

2232860

SPECIFICATION

Conditional-access broadcast transmission

The present invention is concerned with conditional-access broadcast transmission of television or radio signals. Usually this will apply to broadcast material for which a charge is made, to ensure reception only by users who have paid the appropriate charge, or who have appropriate credit facilities.

One example is subscription television – as envisaged on the proposed direct satellite broadcasting services (DBS). A subscription channel will carry scrambled signals that can be recovered only by users who have paid an additional charge. Such a charge might, for example, be in the form of a monthly subscription, or there might be a two-tier system, in which the subscription would cover most programmes, with an additional payment for one or two special programmes during the month.

The DBS proposals envisage the transmission of at least one channel which is open to all and one channel which is accessible only to subscribers. It is convenient to apply a scrambling operation to both types of transmission. For the free-access channel, the key required for descrambling would be freely available, whereas for the conditional-access (subscription) channel the method of descrambling would be secure.

The term "scrambling" used in this specification is intended to describe the processing to which the transmitted signals are subjected in order to render them wholly or partially unusable in their scrambled form. A complementary descrambling process is used at the receiver to recover the original signals. It is regarded as essential that the received signals should show no impairment attributable to the scrambling and descrambling processes. Scrambling may be total, when no sign of the original signal may be detected, or it may be partial in which case, for example, the original picture may be discernible to a limited extent.

The term "encryption" is used in this specification to describe a coding operation which is dependent upon a key. In one possible method an encrypted control data signal is transmitted along with the scrambled picture and/or sound signals, so as to enable a receiver to descramble and reproduce the picture and sound signals. At the receiver, the data signal is decrypted using a secure key, from which a flow of instructions or control signals passes to a descrambling circuit so as to recover the original signals.

Alternatively, the control data signals can be transmitted without being encrypted, but instead an encryption operation is applied to the scrambling control signals at the transmitter. In this case the receiver contains a like encryption system so that the received control data signals are subjected to the same coding operation before being applied to the descrambling circuits. In this way a reversible encryption system is not required.

An important part of a conditional-access television system is the back-up organisation necessary for the payment and validation of reception. The basic needs are to preserve security, to provide a 'user-friendly' operation, and to minimise the size of the back-up organisation.

A first possibility is that payment and hence validation of reception will be made in advance; however, there may be more than one level of payment, as stated above. Options can be kept open for pre-payment for special programmes, which would not necessarily mean a commitment to particular special programmes but could be in the form of credit that could be expended on any programmes of this kind at short notice; a for of 'impluse-buying' would thus be permitted, although using pre-purchased credit. In a similar way, a telephone (viewdata) debiting method could be developed. In this case, there need not necessarily be pre-payment but a direct debiting method could be used.

In the following description it is assumed that both video and sound signals will be scrambled, and that the sound signals will be transmitted in digital form. Possibly a six-channel 2048 kbit/s digital sound multiplex will be adopted. In this, a pair of television sound signals will be carried in the six-channel multiplex digital sound signal structure. If only the television sound signals are to be scrambled, this must take place before the signals are multiplexed; similarly, in the receiver, the descrambling process must then follow the demultiplexer. The method to be used for scrambling the digital sound signal is immaterial for the purpose of the present specification. The other four channels available in the sound multiplex structure may be used for radio signals or for digital data (e.g. tele-software).

One possible method of scrambling the picture signal is to cut each television line signal into two parts at a selected one of, say 256 defined points in time along its duration, according to a pseudo-random sequence, so that the cut may occur at a different randomly-selected point along each line. The two sections of the line signal are then transmitted in reverse order, and a thoroughly scrambled picture is found to result.

Descrambling the received signals requires storage and time-shifting of the picture signal and this is believed to be possible using charged-coupled devices (c.c.d's). Alternatively digital processing could be used. A preferable approach to the descrambling problem, in this case, seems to be through the use of digital signal processing within the domestic receiver itself.

The system chosen should be designed to make illegal descrambling as difficult as possible. Two basic approaches are open to a potential pirate. He can attempt to reconstruct the original picture or sound signal using only the scrambled signals themselves and independently of the encrypted control signals. In some cases, such as with the scrambling system described above, this would be a formidable task indeed. Alternatively, he can attempt to find the key and thereby derive the control signals for the descrambling circuits to recover the original signals.

Consideration has been given to a number of known existing pay-television schemes, but none has been

found suitable in the case of a very large number of potential subscribers (approximately 10 million in the United Kingdom). Many systems of pay-television (e.g. in the United States of America) use personal user addressing in which a unique number is assigned to each receiver. Provided the user has paid his subscription, his number is incorporated in the broadcast transmissions and his receiver is thereby 'enabled' and descrambles and reproduces the signals. In an alternative method, the personal numbers of those subscribers who have failed to pay the charge are transmitted and their receivers are thereby disabled; this has the advantage of 'failing safe' so that no subscriber who has paid his subscription should find his receiver not delivering the expected sound and picture. For the United Kingdom, with 10 million potential subscribers, a personal user addressing system would be impractical. By way of illustration, it may be assumed that about 40 bits would be needed for each customer, comprising the customer's address number and his personal identification number (PIN). To permit reliable reception, about 100 bits would need to be transmitted. A data channel with a capacity of 100 kbit/s would then need slightly more than 2¾ hours to transmit this information. This could represent an unacceptable delay in validation.

Other methods of encryption involve either a special unique decryption device attached to the receiver, or the receiver embodies an 'enabling' switch (which may be real or notional) and which is thereby inherently less secure.

The invention is defined in the appended claims, to which reference should now be made.

The invention will be described by way of example with reference to the drawings, in which:-

Figure 1 is a block diagram of a television receiver embodying the invention;

Figures 2, 3 and *4* show different removable conditional-access sub-systems (CASSs) which can be used with the receiver of Figure 1;

Figure 5 illustrates part of the CASS of Figure 2 in more detail;

Figure 6 illustrates a ground station;

Figure 7 illustrates a CASS and PIN receiver for use with the ground station;

Figure 8 illustrates a computer for use with receivers of the type shown in Figure 7;

Figure 9 illustrates a pre-payment receiver for use with the ground station of Figure 6;

Figure 10 illustrates a computer for use with receivers of the type shown in Figure 9;

Figure 11 illustrates a receiver in relation to the receiver/CASS interface; and

Figure 12 illustrates possible forms of encryption control data transmitted over-air.

It is useful first to look at the proposed method from the point of view of the user. It is assumed that all the DBS equipment has been installed and operates satisfactorily on non-scrambled signals. The following sequence could then occur.

(i) The user would make his first payment.

(ii) He would then receive, by post, a conditional-access sub-system (CASS) that would slot-in to his receiver (or adaptor).

(iii) The user would also receive by separate letter a Personal Identification Number (PIN) and he would enter this number into the receiver via key-pad or other means. The receiver would then reproduce the descrambled picture and sound signals.

(iv) Further payments, say at monthly intervals, will result in the issue, by post, of new PIN's which the user will key-in to maintain his service.

(v) Failure to make a due payment will result in no issue of a new PIN with consequential cessation of the service, and the appearance of scrambled picture and sound, on expiry of the current PIN. Subsequent payment will result in the issue of a new PIN which can be entered to restore the lost service.

Referring now to the drawings Figure 1 shows a broadcast television receiver incorporating a descrambler 10, and Figure 2 shows a decrypter conditional-access sub-system (CASS) 30 which can be used in the receiver. In the receiver of Figure 1, DBS signals are received at an antenna 1 and applied to a down converter 2, and demodulated baseband signals emerge from a tuner unit 3. The digital sound signals need first to be de-multiplexed in a digital demultiplexer 4, but then the video and digital sound signals are descrambled in respective descrambler circuits 11, 12 and passed to the appropriate picture and sound reproducing circuits.

In an adapter a descrambler 10 is also included but in that case a UHF modulator 16 is provided for application to the antenna socket of a conventional UHF receiver. As shown there are two sound channels which are separated in a sound decoder 17 and applied to respective digital-to-analogue converters 18. The two sound signals may be the two channels of a stereo sound system or may represent two languages for example.

The CASS 30 includes decryption means e.g. in the form of a "Data Encryption Standard" (DES) chip 31 (see, for example, USA, 1977, "The Data Encryption Standard" Federal Information Processing Standard No. 46, issued by U. S. Department of Commerce and U. S. National Bureau of Standards, 15th January 1977). Decrypter operation may be summarised as follows:

(a) When the DES chip 31 is supplied with the correct DES key input (on line 32) this enables it to decrypt the input encrypted descrambling control signal fed via connections such as interfaces 33, 15 from a data decoder 13 in the receiver. It is assumed that the control signal was encrypted at source, using the same key, and transmitted in multiplex form with the sound and other data signals.

(b) The DES chip then delivers descrambling control signals, via the interfaces, to the two descrambling circuits 11, 12 and the original video and sound signals are recovered.

(c) The correct DES key is obtained from a matrix unit 34 whenever both the correct CASS code from a CASS code store 35 and the related PIN from keypad 14 are supplied as inputs to it. The DES chip provides an encryption system that is highly resistant to attempts to find the key, as discussed in the above-mentioned reference. There are 2^{56} possible keys so that, for example, making 1,000,000 co-ordinated attempts per second simultaneously using 1,000,000 DES chips, it could take many hours to find the correct key.

(d) The PIN is the current value entered by the user using the keypad 14 or some alternative input device, e.g. a light pen. The PIN could conveniently be a seventeen-digit decimal number, perhaps structured to help to reduce errors on entry.

(e) The CASS code is selected by the off-air data (control lines 36) from a set of CASS codes stored on the decrypter card.

(f) The CASS codes are unique to each user, and are programmed-in by a central computer. The CASS is posted (by the computer) to the user; the posting of a new CASS to a user will be an event that may take place only at intervals of several years.

(g) When an appropriate payment has been made, the same computer will post a letter to the user giving him his new PIN, (in the case of a two-tier payment system two PIN's would be supplied). This PIN can be entered immediately, when it will be stored, but it will not become effective until a new CASS code is selected (on receipt of off-air data), when the old PIN will become reduntant. This will probably be at the end of the month (assuming a monthly routine). The DES key will also probably be changed at this time.

(h) The entering of a new PIN in advance of the date of usage will require validation to re-assure the user.

(i) The DES key can be changed at other times by the broad-casting authority without changing any PIN (as an anti-piracy measure to improve security).

In other words, to operate the descramblers it is necessary to provide decrypted descrambling control signals which at least for the video descrambler 11 will contain an 8-bit code. The decryption operation is effected by the DES circuit 31 on the broadcast encrypted descrambling control signals, in response to a DES key signal on line 32. Also transmitted is a "which CASS code" signal which changes, say, each month. All these signals just mentioned are the same for all users of a CASS of the type shown in Figure 2, i.e. for all subscribers.

Each individual subscriber, however, has a different set of CASS codes stored in the CASS code store 35. Each CASS code has associated with it a PIN so that when the individual CASS code is combined with the correct undivided PIN in circuit 34 the appropriate key is generated on line 32.

The stored code would, of course, be different for different users. As shown at least the code storing means is, or is part of, a removable unit. Although it could be stored in magnetic form (like a bank card), preferably it forms part of a plug in card. The key code identifies to the deciphering means the cipher currently being used. The code storing means contains a plurality of stored codes selectable under control of broadcast signals.

It may be noted that:

(a) All receiver descrambling and decryption circuits can be identical and need not be confidential to preserve security.

(b) The day-to-day running of the system could be almost entirely computer-operated, although means would have to be provided to interface between the computer and the payment points (such as for bank standing orders). There would also need to be arrangements to deal with lost or faulty cards, etc.

(c) The CASS 30 would contain all the necessary LSI circuits to carry out its functions. Even if a set of CASS codes could be obtained by breaking open a card (or by other means), it is difficult to see how a sustained piracy operation could be maintained.

(d) The overall data-rate required for the encrypted descrambling control signals should be well within the available data-channel capacity in the digital sound multiplex.

(e) At any one time, the DES key will be the same within all the CASS circuits.

The CASS code store 35 is a ROM. The matrix 34 is a processing unit for combining the CASS code and the PIN signal by a process such as addition, multiplication, division, etc. or possibly some more complicated process, such as one involving encryption and decryption in which the matrix would itself be a DES or similar circuit. Figure 5 shows an example of this. In Figure 5 the circuitry is shown in more detail, in that the relevant buffer registers are shown. The encrypted descrambling control signals of 64 bits received from interface 33 are held in a register 20 for application to the DES circuit 31. A 10-bit 'which CASS code' signal also received from the interface 33 is applied to the CASS code store 35 which outputs a 56 bit CASS code to a CASS code register 21. The PIN is transferred from interface 33 to a PIN register 22. The matrix 34 is formed by a DES circuit and the output of circuit 34 is held in a DES key register 23 for application to DES circuit 31. The output of DES circuit 31 is applied to a register 24 and thence to a descrambling control signal generator 25 which provides descrambling control signals containing e.g. 8-bit codes. A single physical DES circuit may be time shared to perform the functions of both circuits 34 and 31.

Although, theoretically, the CASS 30 could consist simply of a single read-only memory, the inputs to such a ROM would typically be a 17-digit (56-bit) PIN, a 64-bit block of coded information and, say, a 6-bit signal defining the card code. The output would be a 64-bit number. Thus the ROM would have to contain $2^{126} \times$ 64-bit words. This size of memory is not realisable. Even if it were and even if it could be read at the rate of 100,000 (64-bit) words per second, it would take 10^{25} years to read the entire contents via the connecting leads. The illustrated arrangement including the CASS-code store and matrix is a realisable alternative to the

ROM. Moreover, the division of operations permits changes to be made in either or both the scrambling pattern and the key. Moreover, the CASS's themselves could be changed from time to time, or if a major breach of security were to occur.

Other forms of CASS are envisaged, such as pre-payment credit CASSs, that could be operated simultaneously with the CASS and PIN systems of Figure 2. Another kind of CASS should include a PRESTEL-type connection to the telephone system which would allow a direct-debiting method of payment to be used.

Thus Figure 3 shows a pre-paid CASS 40. The circuit 50 in Figure 4 shows one method of connecting to a direct-debiting telephone system. As an alternative, both the CASS key and the PIN could be obtained via the telephone line. The decrypter circuit shown on this CASS could also employ a DES circuit, or a circuit of that kind.

Thus, in the "pre-paid CASS" 40 of Figure 3 the DES circuit 41 is supplied with a key code from a key store 47 under off-air control (signals 46), provided that a credit register or counter 48, which is decremented during use (if desired, at a variable rate according to the nature of the programme material as indicated by off-air control signals 49), indicates remaining credit. A credit display circuit may be provided within the receiver. The CASS must, of course, be exchanged for a fresh one when the credits are fully used.

The telephone link conditional-access sub-system has a DES circuit 51 whose key is provided by a decryption circuit 59 responsive to signals received via telephone line interface 60, which also reads a debit register 61. The telephone link may provide a direct debiting facility to the user's bank account.

Figure 6 shows one possible form of ground station for the DBS system. The ground station includes a truly random number generator 70 which is applied to a 'pseudo-random sequence parameters and initial conditions generator' circuit 72. Circuit 72 also receives start signals from an initialisation circuit 74 controlled by signals from a computer (Figure 7). Circuit 74 thus generates control data which is applied to a pseudo-random sequence generator 76 which applies a sequence to a scrambling control circuit 78 which controls a scrambler 80 in the digital sound signal path. A scrambler 82 is included in the video signal path, the similar control chain for this being omitted for clarity.

The control data from circuit 72 is also encrypted in a DES circuit 84 and multiplexed with the digital sound/data channel in multiplexer 86. The DES circuit 84 receives the current key from the computer over a protected link. The output of multiplexer 86 is modulated in a modulator 88 onto a subcarrier and added in an adder 90 to the scrambled video signal for application to transmitter circuits 92. The broadcast transmission from antenna 94 is then received by satellite 96 and returned to earth for reception by the users. As the control of the scrambling is by means of pseudo-random sequences whose parameters and timing are varied from time to time under the influence of a (truly) random number generator, although the actual parameters and timing of each pseudo-random sequence will be determined and changed arbitrarily, the decrypted control data will enable a receiver to replicate the correctly timed sequence for use in the descrambling circuits.

Figure 7 shows a 'CASS and PIN' type of receiver based on Figures 1 and 2 for use with the station of Figure 6. Similar references are used as previously and a detailed description is not therefore given separately. In this instance an external keypad or other input device is used in conjunction by a PIN store circuit 100 and PIN select circuit 102 which is controlled by data detected by the data decoder 13.

Figure 8 shows that part of a computer installation associated with the ground station of Figure 6 and receivers of Figure 7.

In the computer, the choice of DES keys is also under the control of a random number generator 110 and the whole process of reproducing CASS's and PIN's is buried in the computer and no human access is needed, except as an input to "enable" the process via a VDU keyboard 112. Areas requiring special security are the current-DES-key register 114 and the DES key link to the ground station.

A select DES key circuit 116 receives control and scheduling information from a source 118 which also feeds the transmitter station. Using the random number generator 110 a DES key is drawn from a store 120. A series of future DES keys is stored in a store 122 and each fed at the appropriate time to the current DES key register 114.

The CASS and PIN issuing circuitry takes these DES keys and using an inverse matrix 124 to the receiver matrix 34 generates appropriate PINs, given the CASS codes which have been generated by generator 126 for each customer. Customer data is held in a store 130 with the individual CASS codes. Appropriate equipment 132 is included for preparing and mailing the CASSs, and likewise equipment 134 prints and mails the PINs.

Figures 9 and 10 show a receiver and the relevant part of a computer installation for a pre-payment system. The receiver of Figure 9 is shown as including a programme logging store 140 in the CASS and display circuits 142 in the receiver proper. The programme logging store 140 is particularly designed for use with a returnable CASS, to enable information on receiver usage to be obtained. In the computer in Figure 10, the next DES key register 122 is connected to a select DES key circuit 150 which is used in the generation of programmes for new CASSs (152) and in the reading and reprogramming of used CASSs (154). The programme information is used to compile viewing statistics (156).

In other respects the pre-payment system is similar to the CASS and PIN system, except that here no PIN exists and the pre-paid cards could be distributed and sold at places such as Post Offices, shops, banks etc. This kind of card would be suitable for multi-tier charging, since facilities could be provided to inform the

user as to the rate for the programme, credit remaining, etc; "impulse-buying" would therefore be possible.

In the systems so far described the control data has been encrypted by the DES circuit 84 prior to transmission. The DES circuit 31 at the receiver then has to effect the converse decryption operation. Alternatively, however, the DES circuit can be used at the ground station to encrypt the control data applied to the pseudo-random sequence generator for the scrambler, as shown at 160 in Figure 6. The control data can then be sent without coding, and the DES circuit 31 at the receiver then effects the identical operation to the circuit 84 at the transmitter. A reversible encryption operation is then not required.

It should also be noted that while a single random number has been illustrated for the scrambling and encryption procedures, separate random number generators could be used for these two operations.

In another modification of the CASS and PIN system, the PIN, which needs to be transmitted relatively infrequently, could be transmitted in the digital data stream. The fact that a long cycle time was required to cover all users would not then matter. Alternatively, users could be catagorised to reduce the time taken for the necessary enabling information to be transmitted.

It might be appropriate to have two PIN's per user, one for a basic service and one for a premium service at greater cost.

In practice it may be desirable to re-initialise the pseudo-random sequence generators at frequent intervals to make it even more difficult for a pirate to receive unauthorised transmissions. A new descrambling control signal would also be used relatively frequently.

One possible interface between the receiver and the conditional-access sub-system will now be described. Figure 11 shows how such a sub-system 200 can be connected to the other elements of the descrambling process which are housed within the receiver 202. The method of picture and sound descrambling is defined by the circuits within the receiver and is common to all broadcasters, but the decryption method and means of payment can be unique to each broadcaster and is defined by plugging in an appropriate sub-system.

There is a need for a universal interface which can communicate with suitably designed sub-systems to provide for various methods of payment. One example will now be given. The sub-system communicates to and from the receiver by means of a bi-directional self-clocking serial digital data bus 204 which uses a single connection with earth return. The maximum transfer rate of this data bus is assumed to be typically around 9 kbytes/sec. Supporting connections are also required viz: power supply 206, 4 MHz microprocessor system clock and synchronising signal source 208; a list of the required connections is given below. There are also options for a special programming voltage for an electrically-alterable read-only-memory, and a direct pseudo-random binary sequence (p.r.b.s.) output if this should become generally preferred. A spare pin is provided, possibly for use by the broadcaster when re-programming the sub-system.

The required connections are as in the following Table 1.

TABLE 1

Details of Connections between Receiver and Sub-System

Pin No.	*Symbol*	*Signal*	*Characteristics*
1	GND	Ground reference	
1	VCC	Supply voltage	5v ± 10%
3	CLK	Clock signal	4 MHz duty cycle 45%–55% rise+fall time 10%–90% 30n high level:2.8v min VCC max low level: Ov min 0.4v max
4	RTM	Reset and time marker	Resistive pull-up on DSS 10K
		Time marker:	Activated by going high and remaining there for greater than 16 clock periods (4μs) and then going from high to low within one clock period.
		Reset:	Activated by remaining high for greater than 256 clock periods (64μs) before going low.
5	SDIO	Serial data input/output	Bidirectional self clocking serial data bus.
6	VPP	Programming bias voltage	Voltage required to program the EAROM used in decryption sub-system (21v at 100 mA max). (The 5v supply on pin 2 may suffice for this purpose).
7	RFM	Reserved for future use.	Pin 7 is reserved for possible future use for the output from the decryption sub-system of a pseudo random sequence clocked by CLK and initialised at times defined by RTM. The feedback and initial condition of this sequence is defined within the sub-system.
8	SPARE		Possible use by broadcasters as programming enable pin. No connection should be made to this pin.

When a 'cold-start' reset signal generated by the receiver is sent to the sub-system, the circuits on the sub-system are initialised and a sequence of instructions is sent on the serial data bus from the sub-system to the sound/data demultiplexer 210. These instructions (which can also be sent at other times where appropriate) are detailed in item 1 of Table 2 which is appended to this description, and are designed to deal with addressing modes, examples of which are shown in Figure 12. They set up the demultiplexer with up to eight data-packet address specifications. The address is specified in terms of a header byte followed by between zero and four further bytes. Subsequently only over-air data with a packet address which conforms to one of these eight address specifications will be grabbed from the transmitted multiplex. As shown in Table 2, the instructions to the demultiplexer also indicate the number of further (message) bytes in each packet types and whether or not a 3 byte check is included. The demultiplexer then error-checks the data where appropriate and the packet address is replaced by a single byte indicating the data source (in this case "off-air") and the address specification to which it conforms. This byte and the message data is then placed in a buffer store ready for transfer to the sub-system at a lower data rate (see item 2 of Table 2).

By this means the very high data-channel rates used for user-addressability systems, or systems

responding to 4 keys out of 3000, can be dealt with despite the much slower transfer rate to the sub-system.

Figure 12 shows the possible formats which over-air transmitted data might take. It should be noted that the formats shown in Figure 12 are simply examples for the purposes of illustration and should not be taken to represent any particular type of system.

The address specification and recognition functions can be handled by a separate module 212 which need only be included when an entire sound channel is used to convey individually-user-addressed data.

Other data which can be sent to the sub-system over the data bus are a personal identification number (PIN) keyed in by the user with the keypad 214 (card and PIN system), a confirmation of willingness to pay for a programme (pay-per-view), and requests for a display (216) of remaining credit or monthly billing information derived from the sub-system's memory. In all cases a preceding byte will indicate the source of the data, see item 5 of Table 2.

The main data output from the sub-system is instructions to the p.r.b.s. generators 218,220. There are two generators one to provide control data for sound descrambling (up to eight channels) and the other for the vision descrambler. Each generator can be set up for its initial condition or its feedback parameters ("key"), to take effect at the next time marker, this being decoded in the sync. decoder 222. Thus four types of instruction are required, see item 3 of Table 2. These instructions include a simple error check so that a re-transfer can be requested in the event of an error.

Time markers can be at intervals of two seconds and are fed to the p.r.b.s. generators and also to the sub-system 200 via the RTM (reset and time marker) pin.

Other data output from the sub-system includes text messages for display to the user which will be sent either following the users request, or when deemed appropriate (e.g. "credit running out"); see item 4 of Table 2.

It can be up to individual broadcasters to decide what use is to be made of the incoming data in up to eight off-air addressing categories, and how this data and user-provided data is manipulated to provide the instructions to set up the p.r.b.s. generators, and then to produce a sub-system to carry out the necessary processing.

The over-air data could include a packet address common to all broadcasting encryption systems in which the message bytes carry details of the subscription system or systems in use of that channel. An example is given at the bottom of Figure 2. This would make it possible to have a universal subsystem which reacts automatically according to the system to which the receiver is tuned.

Table 2 summarises the types of instruction and data to be carried by the digital data bus and estimates the required data rate. It is apparent that a transfer rate of 9600 baud should suffice if the p.r.b.s. generators are updated at two second intervals. If security considerations were to indicate that more frequent updating is required, then a higher transfer rate would be needed.

TABLE 2

List of types of instruction on digital data bus

No.	*Route*	*Content*		*Bytes*	*Typical Rate of use* (Instructions/Period)	*Approx. Bytes/Sec During use*
1	Sub-system to Sound/ data Demultiplexer	Routing/Instruction		1	8 at switch-on	60 during first second after switch-on
		Which address specification store	(0–7)	⅜		
		Error check included	(Y/N)	⅛		
		Address specification				
		Header byte		1		
		Number of address bytes	(0–4)	¼		
		Address bytes		0–4		
		Number of message bytes	(0–15)	½		
		Transfer Error check		1		
		Max. length		8¼		
2	Sound/data De-multiplexer to Sub-system	Routing/Instruction		1	EH1 10/sec(see Fig.1)	120
		Which address specification matched	(0–7)	⅜	EH2 1/hour	
		Number of message bytes	(0–15)	½	EH3 15/30 secs.	
		Message bytes		0–9	EH4 1/2 secs.	
		Transfer Error check		1		
		Max. length		12⅞		

TABLE 2

List of types of instruction on digital data bus

No.	*Route*	*Content*		*Bytes*	*Typical Rate of use* (Instructions/Period)	*Approx. Bytes/Sec During use*
3	Sub-system to prbs generators	Routing/Instruction		1		
		Which generator (sound vision)		⅛	4/2 secs	25
		key or initial conditions		⅛		
		data		8		
		Transfer error check		1		
		Total length		11¼		
4	Sub-system to display device	Routing/Instruction		1	1/user request	100 only when writing to display
		how many bytes	(0–63)	¾	1/week (warnings)	
		data bytes		0–63	1/switch-on	
		Transfer error check		1		
		Max. length		65¾		
5	User Keypad to Sub-system	Routing/Instruction		1	1-17/PIN entry	20 only whilst keying in data
		how many bytes	(0–63)	¾	1/user request	
		data bytes		0–63		
		Transfer error check		1		
		Max. length		65¾		

Total data transfer requirement when all types of instruction are active during a 2 second period = 325 bytes/sec. (2600 bits/sec)

Allowing for overheads (start bits stop bits, guard bands, etc.) and fr re-transfers due to errors an overall baud rate of 9600 baud would seem to be appropriate for the digital data bus.

CLAIMS

1. A broadcast communication receiver for scrambled signals, having:-
a descrambler responsive to control signals to descramble the received signal;
control signal extraction means for extracting from the received signal descramble control signals transmitted therewith;
cryption means subjecting the control signals to a cryption operation to provide a signal for application to the descrambler; and
enabling means for enabling the cryption means, the enabling means being arranged to store at least one code and to enable the cryption means with a key dependent upon said stored code in response to two enabling inputs to the enabling means.

2. A broadcast communication receiver for scrambled signals, having:
a descramber responsive to control signals to descramble the received signals;
control signal extraction means for extracting from the received signal descramble control signals transmitted therewith;
cryption means for subjecting the control signals to a cryption operation to provide a signal for application to the descrambler; and
enabling means for enabling the deciphering means and comprising means storing at least one code, means for manual input of an identification code, and means for combining the two codes to produce a signal enabling the cryption means only in the event of a predetermined correspondence between them.

3. A broadcast communication receiver for scrambled signals, having:
a descrambler responsive to control signals to descramble the received signals;
control signal extracting means for extraction from the received signal descramble control signals transmitted therewith;
cryption means for subjecting the control signals to a cryption operation to provide a signal for application to the descrambler; and
the cryption means being responsive to a key code identifying the cipher used; and the receiver further being provided with:
means storing a plurality of key codes and responsive to transmitted signals to select one, and means for measuring the amount of use of the system and for disabling the deciphering means when use reaches a predetermined limit.

4. A broadcast communication receiver for scrambled signals, having:
a descrambler responsive to control signals to descramble the received signals;
control signal extraction means for extracting from the received signal descramble control signals transmitted therewith;
cryption means for subjecting the control signals to a cryption operation to provide a signal for application to the descrambler; and
the cryption means being responsive to a key code identifying the cipher used; and the receiver further being provided with means for connection to a telephone line for producing the key code in response to signals received over the telephone line.

Printed for Her Majesty's Stationery Office, by Croydon Printing Company Limited, Croydon, Surrey, 1984.
Published by The Patent Office, 25 Southampton Buildings, London, WC2A 1AY, from which copies may be obtained.